

CLERK'S OFFICE

A TRUE COPY

Nov 03, 2020

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)The Cellular Telephone Assigned Call Number  
(330) 881-9987

Case No. 20 MJ 212

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A.

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2314	Transportation of Stolen Goods in Interstate Commerce
18 U.S.C. § 371	Conspiracy to Commit Offense Against the United States

The application is based on these facts:

See affidavit attached.

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

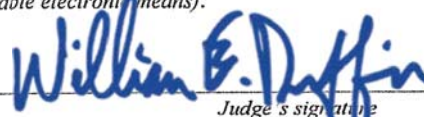


Applicant's signature

FBI SA Eric P. Fraser

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone (specify reliable electronic means).

Date: November 3, 2020City and state: Milwaukee, WI


Judge's signature

U.S. Magistrate Judge, William E. Duffin

Printed name and title

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT

I, Eric P. Fraser, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **(330) 881-9987** (the “Target Cell Phone”), whose service provider is T-Mobile (“Service Provider”) a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phone .

3. I am a Special Agent with the Federal Bureau of Investigation and have been since March 2008. I am currently assigned to the North Central High Intensity Drug Trafficking Area (“HIDTA”) Office (since January 2020). As such, I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony

offenses. I have participated in numerous complex narcotics, money laundering, violent crime, armed bank robbery, and armed commercial robbery investigations that implicate the provisions of Title 18 and Title 21 of the United States Code. I have employed a wide variety of investigative techniques in these and other investigations, including, but not limited to, the use of informants, wiretaps, cooperating defendants, recorded communications, search warrants, surveillance, interrogations, public records, DNA collection, and traffic stops. I have also received formal training regarding the same.

4. This affidavit is based upon my personal knowledge, my training and experience, and on information reported to me by other state and local law enforcement officers during the course of their official duties. This affidavit is also based upon police reports, electronic and physical surveillance, physical evidence, electronic evidence, and witness statements that I consider to be reliable as set forth herein. The facts below are based upon information obtained from my investigation, as well as information I have received from other law enforcement officers. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that JAMES PATRICK QUINN has violated Title 18, United States Code, Section 2314 (Transportation of Stolen Goods in Interstate Commerce) and Title 18, United States Code, Section 371 (Conspiracy to Commit Offense Against the United States). QUINN was charged by Criminal Complaint with these crimes on November 3, 2020 and is the subject of an arrest warrant issued on November 3, 2020. There is also probable cause to believe that the location information

described in Attachment B will assist law enforcement in arresting QUINN, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

6. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. The United States, including the Federal Bureau of Investigation, is conducting a criminal investigation of QUINN regarding possible violations of 18 U.S.C. § 2314 and 18 U.S.C. § 371.

8. On the morning of July 12, 2016, the City of Brookfield Police Department responded to a burglary that had occurred overnight at Treiber & Straub Jewelers (14740 W. Capitol Drive, Brookfield, Waukesha County, Wisconsin). The burglars entered the jewelry store by cutting the phone and cable lines, removing light bulbs from exterior lights, spraying foam into external audio alarm systems, and prying the back door open. The burglars then disabled the interior alarm system and cut a hole into the vault using sledge hammers and power tools. They took over \$7 million in jewelry, diamonds, watches, and other items. Surveillance footage captured these events. On July 11, 2016, between approximately 7:36 p.m. and 7:52 p.m., an individual is seen on exterior video surveillance approaching and leaving the northwest corner of the business, which is near the area where the internet/cable lines were cut. This took the alarm/server offline. Between approximately 10:49 p.m. that evening and 4:35 a.m. on July 12, three individuals are seen on external and internal video surveillance breaking into the business and carrying out the burglary as described above. The video shows two of the three suspects using cellular phones at

various times. The suspects are not seen on video surveillance after approximately 4:35 a.m. on July 12, 2016.

9. On July 12, 2016, while officers of the Brookfield Police Department (BPD) were processing the burglary scene, blood was located inside the store on the exterior of the employee-only women's restroom door and collected as evidence. Evidence was submitted to the State of Wisconsin Crime Lab. After laboratory analysis, the DNA was not identified in the Combined DNA Index System, but it was determined that the unknown sample is from a male individual.

10. Approximately one year prior to the burglary, on July 29, 2015, the City of Brookfield Police Department received a call from Treiber & Straub regarding an incident involving two individuals who were observed via video surveillance cameras carrying flashlights and peering into the business's windows at approximately 4:15 a.m. The surveillance camera captured a close-up picture of one of the two individuals as he peered into the business window using a flashlight. They were observed, via external video surveillance cameras, loitering in the back of the business until approximately 5:00 a.m. on July 29, 2015. Both men were white males who appeared to be in their 30s or 40s. Based upon the suspicious nature of this incident, law enforcement officials believe the two individuals observed on the video surveillance during the early morning hours on July 29, 2015, were either casing the business or intended to burglarize the business.

11. On September 14, 2015, a citizen at a residence to the north of Treiber & Straub Jewelers observed two male individuals acting suspiciously in a wooded area that separated the citizen's property from Treiber & Straub's property. A citizen used a flashlight to locate the subjects at which time the subjects fled the area on foot. The citizen notified the City of Brookfield

Police Department of the above information, however, officers were unable to locate anyone on foot in the area.

12. The following morning, on September 15, 2015, Treiber & Straub employees opened the store for business and found the store had no phone or internet connections. The phone/internet provider was contacted and a technician attempted to diagnose the problem at the store. The technician found the internet/phone lines had been cut under ground level in the northwest external corner of the business. That area of the business was found to be in close proximity to the area where the citizen witness observed the two suspicious male individuals.

13. On July 16, 2019, I traveled to the Youngstown, Ohio area with Brookfield (WI) Police Department Detective Michael Skemp. There, we met with local law enforcement officials regarding the Treiber & Straub incidents from both 2015 and 2016. The local investigators were from the FBI's Youngstown Resident Agency, Ohio Bureau of Criminal Identification and Investigation, Boardman Township (OH) Police Department, and Canfield (OH) Police Department. Still photographs from the above-mentioned video surveillance of two white males "casing" the store July 29, 2015, were shown to local investigators. Based on their review of these images, they identified one of the subjects as F.S. and the other subject as QUINN. F.S. and QUINN are known to law enforcement as professional burglars from the Youngstown, Ohio area. They are known to travel throughout the United States committing jewelry store burglaries. Local investigators were also shown video surveillance from the July 11-12, 2016 Treiber & Straub burglary; they indicated that the modus operandi was similar to F.S.'s previous burglary jobs. F.S.'s criminal history shows approximately 25 arrests between 1982 and 2014. The arrests include multiple counts of theft, breaking and entering, safecracking, criminal trespass, burglary, receiving stolen property, bribery, and other offenses. QUINN's criminal history shows approximately 11

arrests between 1993 and 2016 and includes multiple counts of theft, breaking and entering, possession of burglary tools, criminal trespass, burglary, receiving stolen property, and other offenses.

14. On July 18, 2019, I sought federal search warrants for buccal swabs from F.S. and QUINN. The warrants were approved and signed by U.S. Magistrate Judge George J. Limbert of the U.S. District Court for the Northern District of Ohio. Case agents obtained buccal swabs from F.S. at his home address.

15. QUINN was on federal supervision at the time, and his probation officer informed me that QUINN's address was 4125 New Road, Youngstown, Ohio. After some initial difficulty locating QUINN, we found him outside of this address. As case agents approached, they verbally identified themselves to QUINN and attempted to inform him of the search warrant. QUINN was in possession of a white object, which he was holding in his hands/arms. QUINN did not comply, and attempted to flee the area on foot. After a brief foot pursuit, QUINN was detained in a wooded area. He was no longer in possession of the white object. A white plastic bag was eventually found partially buried under a log in the wooded area, close to where QUINN was now detained. QUINN denied any knowledge or ownership of the bag or its contents. The bag and its contents were therefore recovered as abandoned property. After executing the oral swab search warrant, QUINN was released.

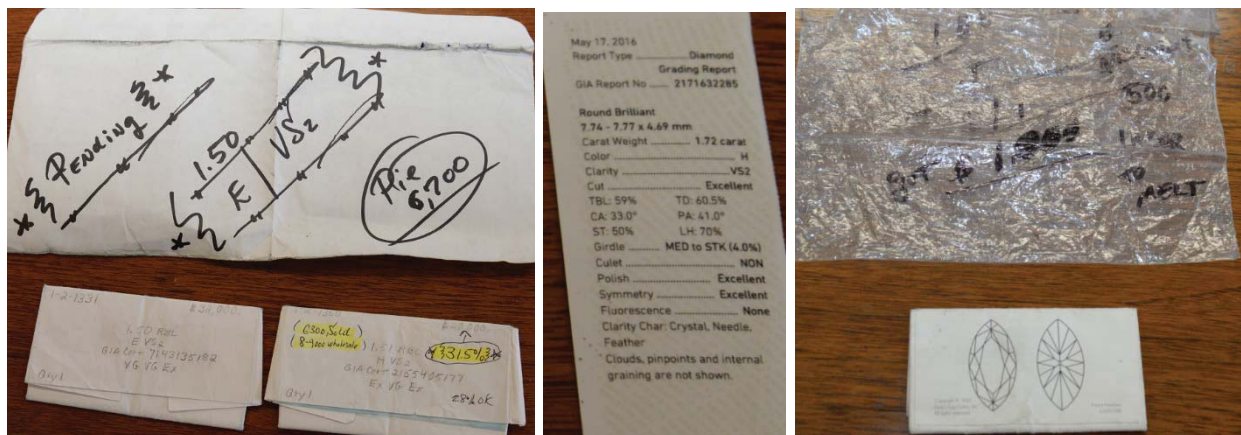
16. The buccal swabs obtained from QUINN and F.S. were submitted for analysis and comparison. To date, no match has been found to the male DNA profile extracted from the blood found on the women's bathroom door at Treiber & Straub after the burglary.

17. The white plastic bag and its contents were brought to the FBI's Youngstown office, where its contents were inventoried. It contained an LG cellular phone Model: LG-B470,



IMEI: 356585091001172; one green in color Huntington Bank bag; one green in color Citizen's Bank bag; a t-shirt; and blue nitrile gloves. The Huntington Bank bag contained \$8712.13 in U.S. currency and scraps of paper. The Citizen's Bank bag contained \$236.20 in U.S. currency, and paperwork including a valid Ohio Driver's license in the name of James Patrick QUINN with QUINN's photo. The paperwork in the Citizen's Bank bag also included a card with the business name "Lexren, LLC" and bank account and routing information. Publicly available records from the Ohio Secretary of State list "James Quinn" as a Member of this Limited Liability Company. I transported all of the items except for QUINN's Ohio Driver's license to the FBI's Milwaukee field office.

18. Also found among the items in the white plastic bag containing Quinn's driver's license were 3 paper envelopes that had writing on them indicating carat weight, cut, clarity and GIA (Gemological Institute of America) report numbers 2171632285, 7143135182, and 2155405177:



19. Based on my training, experience, and information gathered during the course of this investigation, these envelopes are consistent with packaging that is used by jewelers to ship and store loose diamonds. The Gemological Institute of America (GIA) performs diamond grading, and a unique grading report number is assigned to all diamonds the GIA grades. The GIA



report number is assigned to a specific diamond at the time the GIA grades the stone and identifies the stone's specific attributes. The GIA report number follows that specific stone indefinitely.

20. On July 19, 2019, case agents contacted C.W., an employee of Treiber & Straub Jewelers, by phone. Detective Skemp provided the above-listed GIA numbers to Wilson so that they could be checked against Treiber & Straub's records of items taken during the burglary. Wilson was able to confirm that diamonds identified with the above-listed GIA numbers were taken during the July 12, 2016 burglary.

21. Case agents sought federal search warrants for QUINN's properties at 4125 New Road and 90 Kenmar Court, Youngstown, Mahoning County, Ohio; and QUINN's truck, a 2000 Blue Chevy S10 2-door truck, Ohio Registration Plate EZM4604, vehicle identification number 1GCCS19W6YK118249. The warrants were approved and signed by U.S. Magistrate Judge George J. Limbert of the U.S. District Court for the Northern District of Ohio. The warrants were executed on September 19, 2019.

22. During the search of 90 Kenmar Court, a residence then under construction, law enforcement seized \$2,450 in cash, as well as two cellular phones: a Samsung Model SM-J120A UD (Serial Number: R58H42PLCDV) which was located on a bucket next to a refrigerator in the garage, and a Samsung Model SM-G360T (Serial Number: R58H137GT6D) which was located on QUINN's person.

23. During the search of the residence at 4125 New Road, officers found, among other things: jewelers' loupes (commonly used by jewelers as a magnification tool to inspect and view items like precious stones and other jewelry), a book titled "Diamonds," a book titled "Superthief," hand-held radios and chargers, a face mask, a ski mask with holes cut out, and a head lamp.

24. The evidence seized during the searches was transported to the FBI's Milwaukee Office. The two Samsung smartphones seized at 90 Kenmar Court were forensically extracted and examined by members of the FBI's Computer Analysis Response Team. The extractions were then made available for review.

25. The contents of the Samsung SM-J120A UD (Serial Number: R58H42PLCDV) included a file titled "Device Users" which showed only one user, identified in the file as "James Quinn." The phone also contained numerous photos of QUINN and personal correspondence in text message and call logs between QUINN and others. Therefore, while it appears that another individual had been staying in the garage at 90 Kenmar Court when this phone was found and seized, the phone's contents attribute the phone to QUINN.

26. Case agents located a file titled "Device Locations" in the same extraction. By way of background, when a cell phone's location setting/service is turned on, applications on the phone may use cellular data connections and locations for certain features and functions. For example, an application may log the GPS coordinates of a captured photograph. Applications may store such information in the phone's internal memory. The "Device Locations" file on the Samsung SM-J120A UD included certain cellular tower location data (including dates and times) from April 2016 onward.

27. Case agents were then able to create a list of tower locations registered in the file. The data included, but was not limited to, location information corresponding to cellular tower connections during the timeframe surrounding the Treiber & Straub burglary.

28. More specifically, the phone contained evidence of connections at or near the following locations, between July 10 and July 12, 2016:

<b>Date</b>	<b>Time</b>	<b>Tower Location (Latitude, Longitude)</b>
July 10, 2016	10:03 a.m.	Youngstown, Ohio (41.06721, -80.70194)
July 10, 2016	6:51 p.m. 6:52 p.m. 6:53 p.m.	Kalamazoo, Michigan (42.25720, -85.54705)
July 11, 2016	6:35 p.m.	Pewaukee, Wisconsin (43.03906, -88.19218)
July 11, 2016	6:36 p.m. 6:37 p.m.	19245 Janacek Court Brookfield, Wisconsin (43.03238, -88.15202)
July 11, 2016	8:33 p.m.	19295 W. North Avenue Brookfield, Wisconsin (43.05938, -88.15175)
July 12, 2016	7:05 a.m. 7:06 a.m.	Libertyville, Illinois (42.32853, -87.91169)
July 12, 2016	6:05 p.m.	3671 Connecticut Avenue Youngstown, Ohio (41.10721, -80.71606)

29. According to Google Maps, the most direct route between Brookfield, Wisconsin, and Youngstown, Ohio, covers approximately 500 miles over roughly 8 hours of driving. This route would include travel on Interstate 94 in southeast Wisconsin and northern Illinois.

30. Case agents used Google Maps to plot GPS coordinates and measure distances with respect to the particular cell tower locations set forth in paragraph 28 above. Of note, the cell tower in Pewaukee, Wisconsin, is approximately 1600 feet from Interstate 94. The distance from the cell tower at Janacek Court in Brookfield, Wisconsin, to I-94 is approximately 850 feet. The cell tower in Libertyville, Illinois is approximately 800 feet away from I-94 as it passes through that area.

31. Investigators in Wisconsin and Ohio have not found any ties between QUINN and Wisconsin or any other personal or business dealings that would explain his cell phone's brief presence in the Brookfield area on July 11, 2016, in the hours before the Treiber & Straub burglary was carried out.

32. On October 28, 2020, case agents interviewed J.L.J., of Austintown, Ohio. She provided a current cellular telephone number (the Target Cell Phone identified above) for QUINN. J.L.J. and QUINN have been in a romantic relationship since the spring of 2016 and see one another almost daily. J.L.J. stated her and QUINN travel to Erie, Pennsylvania, together on the weekends to visit QUINN's daughter and recently went on a trip together to Atlantic City, New Jersey. QUINN frequently spends the evenings at J.L.J.'s residence, and they frequently communicate via cellular phone.

33. In sum, there is probable cause to believe that QUINN has violated Title 18, United States Code, Section 2314 and Title 18, United States Code, Section 371; an arrest warrant for QUINN has issued on November 3, 2020 from the U.S. District Court for the Eastern District of Wisconsin; and there is probable cause to believe that the location information described in Attachment B will assist law enforcement in locating and arresting QUINN.

34. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

### **Cell-Site Data**

35. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

### **E-911 Phase II / GPS Location Data**

36. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data. Based on my training and

experience, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

### **Pen-Trap Data**

37. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

### **Subscriber Information**

38. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent



or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators.

### **AUTHORIZATION REQUEST**

39. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

40. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

41. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

42. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target

Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and/or flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

43. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

## **ATTACHMENT A**

### **Property to Be Searched**

1. Records and information associated with the cellular device assigned call number **(330) 881-9987** (referred to herein and in Attachment B as “the Target Cell Phone”), with unknown listed subscriber(s) that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the “Provider”), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.
2. The Target Cell Phone.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period **October 15, 2020, to the Present**:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address);
  - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:
  - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - (ii) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received).
- b. Information associated with each communication to and from the Target Cell Phone for a period of **30 days** from the date of this warrant, including:
  - i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
  - ii. Source and destination telephone numbers;
  - iii. Date, time, and duration of communication; and
  - iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication.

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with the Target Cell Phone.

- c. Information about the location of the Target Cell Phone for a period of **30 days** during all times of day and night. “Information about the location of the Target Cell Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
  - i. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider’s services, including by initiating a signal to determine the location of the Target Cell Phone on the Provider’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The

government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

- ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2314 involving JAMES PATRICK QUINN during the relevant time period.

All information described above in Section I that will assist in arresting JAMES PATRICK QUINN, who was charged with violating 18 U.S.C. § 2314 and 18 U.S.C. § 371 on November 3, 2020, is the subject of an arrest warrant issued on November 3, 2020, and is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS**  
**PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-Mobile, and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of T-Mobile. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-Mobile and they were made by T-Mobile as a regular practice; and

b. such records were generated by T-Mobile electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-Mobile in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by T-Mobile, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature